Approved For Release 2006/05/25 : CIA-RDP84B00049R000501150011-3

STAT

News Bulletin

15 September 1982
Item #1

Item from BUSINESSWEEK, dated 20 Sept, page 77.

Kremlin spies target U.S. electronics knowhow

Soviet efforts to steal advanced technology are entering a menacing new phase, one threatening many companies that until now have been unlikely targets for espionage. While Russian spies undoubtedly will continue to chip away at military secrets, they also are spreading their nets much wider, searching for more basic industrial technologies, such as production knowhow for electronics—and they are targeting many smaller, more vulnerable companies.

To obtain this knowhow, the Soviet Union's worldwide intelligence network recently has gone through an unprecedented expansion. The number of technology collection officers has nearly doubled, to an estimated 5,000 agents, and U.S. counterintelligence officers believe most of these new agents are assigned primarily to industrial "beats." Few of the new Soviet technology agents operate as spies in the classic cloak-and-dagger sense. Instead, they function more like market researchers, obtaining information by careful literature searches and trade show visits.

According to the Central Intelligence Agency, three of the Kremlin's top 10 espionage targets now are: anything related to microelectronics; computer knowhow, especially in software and supercomputers; and materials technology, particularly advanced composites. The addition of so many new agents is taken by the CIA as a sign that the Kremlin is keenly worried about its ability to maintain even a semblance of parity with the U.S. in an era when the quality of weapons is more important than the quantity.

Tomorrow's weapons

The U.S. semiconductor industry is on the verge of jumping to a new generation of chips, and the qualitative difference will be far greater than any past transition. These chips, known by such acronyms as VHSIC and VLSI, will provide tomorrow's "smart" weapons with astounding new capabilities. The Soviet semiconductor industry, by comparison,

(OVER)

Approved For Release 2006/05/25 : CIA-RDP84B00049R000501150011-3

Approved For Release 2006/05/25 : CIA-RDP84B00049R000501150011-3

is based largely on outdated equipment pirated from the West. So Soviet leaders are eager to get their hands on as much new equipment as possible—and quickly.

Stealing technology is hardly a new concept for the Soviets, of course. The ruling clique within the Kremlin decided about 15 years ago "to make a concerted effort to rely on the West's proved science and technology," says an official in the Federal Bureau of Investigation's Intelligence Div. "It saves them lots of research and development time and money" that otherwise would have to be diverted from the military sector.

The program is managed with chilling efficiency. The Soviet State Committee for Science & Technology (GKNT) coordinates the effort and determines priorities. The state committee first tries legal means, using East-West exchanges and tours of university and company laboratories—or, when necessary, allocating scarce hard currency to buy a key piece of technology. "There is no such thing as a Soviet scientist coming to the U.S.

The Soviet intelligence net is shifting from the military to industry

to get general information," says the FBI official. "He is, in fact, tasked to come and get a certain piece of information."

When all else fails, the GKNT resorts to clandestine methods and assigns technology targets to either the KGB or a lesser-known intelligence service, the Chief Intelligence Directorate of the Soviet General Staff (GRU). These agencies may in turn enlist the help of their counterparts in an East bloc country, where a favorite ploy is working through a dummy company. Two dozen East European companies are known KGB or GRU conduits. "This [front-company] threat is very clearly increasing, and we can document this," says the FBI source. "But those figures are classified."

"Manufacturing technology has moved to the top of the Russian wish list," says John D. Shea, president of Technology Analysis Group Inc., a San Jose (Calif.) consultant to the Defense Dept. The latest semiconductor fabrication equipment, he explains, could probably cut by half the time it takes for the Soviets to move a new weapon from the drawing board to the battlefield. G. Dan Hutcheson, vice-president of VLSI Research Inc., a semiconductor industry consultant, adds that "Soviet attempts to get this equipment is a real problem—and there is no solution in sight."

Almost 30% of all U.S. chipmaking equipment is exported. But once this equipment leaves the U.S. with an export license, it has a "nasty habit" of showing up on the used-equipment market within a few months, says Hutcheson. The NATO allies make no attempt to regulate the sale of used equipment, so it is a wide-open market for East bloc buyers. Over the past 10 years, the Soviets have obtained hundreds of pieces of semiconductor equipment worth hundreds of millions of dollars, the CIA says, either by clandestine means or through used-machine purchases.

What the Russians can do with Western technology is all too clear. In 1972, Bryant Chucking Grinder Co. sold 164 precision grinding machines to the Soviet Union—over stern protests from the U.S. intelligence community, because the machines turn out precision ball bearings. By the end of the decade, the Defense Intelligence Agency credited the machines with giving the Kremlin the capability of producing far more accurate missile guidance systems. That in turn touched off the U.S. response to "harden" its missile silos and then to devise the controversial MX basing scheme—involving vast expenditures that could have been avoided by more prudent export policies.

Ironically, U.S. industry may be at a turning point in security-consciousness because of the recent "Japscam" revelations. Many companies that never gave espionage a thought are "going through some tough soul-searching," says Donn Parker, a security expert at SRI International. An FBI-sponsored program to brief companies about espionage threats is suddenly popular among Silicon Valley companies with no defense contracts. Says John O'Loughlin, manager of security at chipmaker Intel Corp.: "Companies themselves have to be the first line of defense—and many are now beginning to wake up to their vulnerability."

Approved For Release 2006/05/25 : CIA-RDP84B00049R000501150011-3